MATHEMATICS OF COMPUTATION
VOLUME 57, NUMBER 196
OCTOBER 1991, PAGES 817–823

IDEAL 9TH-ORDER MULTIGRADES AND LETAC'S ELLIPTIC CURVE

C. J. SMYTH

Abstract. By showing that the elliptic curve $(x^2 - 13)(y^2 - 13) = 48$ has infinitely many rational points, we prove that Letac's construction produces infinitely many genuinely different ideal 9th-order multigrades. We give one (not very small) new example, and, by finding the Mordell-Weil group of the curve, show how to find all examples obtainable by Letac's method.

1. Introduction

Letac gave an ingenious construction for 'ideal 9th-order multigrades,' that is, for solutions $\{\{n_1, \dots, n_{10}\}, \{m_1, \dots, m_{10}\}\}$ in integers of the system of equations

$$(1) \qquad \sum_{i=1}^{10} n_i^j = \sum_{i=1}^{10} m_i^j \qquad (j = 1, \dots, 9)$$

with $\{n_1, \dots, n_{10}\} \neq \{m_1, \dots, m_{10}\}$. His method is described in Gloden [4, pp. 54–55] (see also §2). Every solution set $\{\{n_1, \dots, m_{10}\}\}$ gives infinitely many other sets by affine transformation: $\{\{an_1 + b, \dots, am_{10} + b\}\}$ is also a solution set. We regard two solution sets as *genuinely* different only if they are *not* related in this way. That an affine transformation of a solution set is again a solution set is immediately apparent from an alternative formulation of (1), namely that

$$(1') \qquad \prod_{i=1}^{10}(T - n_i) - \prod_{i=1}^{10}(T - m_i) = C \neq 0,$$

where C is independent of T.

The purpose of this note is to show that Letac's method gives infinitely many genuinely different solutions. In fact, Gloden [4, p. 55] implied that the method produced infinitely many solutions of (1). As E. M. Wright [8] points out, however, it is not clear whether or not he meant infinitely many genuinely different solutions. Indeed, Wright remarks that no solution set genuinely different from Letac's example ((6), below) seems to have appeared in the literature. In §3 we give such an example.

Received August 10, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D72, 11G05.

In §5, we compute the Mordell-Weil group of Letac's elliptic curve ((3), below) associated with Letac's method. As a result, we can in principle compute all multigrades (1) obtainable by Letac's method.

2. Letac's method

Letac's method depends on obtaining integer solutions (n, p, q, m) to the equation $((\gamma')$ of [4, p. 55])

$$m^2(1089p^2 - 1053n^2) = q^2(13p^2 - 9n^2). \tag{2}$$

We paraphrase his method by writing $u = 3n/p$ and $v = q/3m$, so that (2) becomes

$$(u^2 - 13)(v^2 - 13) = 48. \tag{3}$$

Then for each rational solution (u, v) of (3), the multigrade system (1) has a rational solution set

$$\begin{aligned}&\{\{\pm 4(u+v), \pm(uv+u+v-11), \pm(uv-u-v-11),\\ &\qquad \pm(uv+3u-3v+11), \pm(uv-3u-3v+11)\},\\ &\{\pm 4(u-v), \pm(-uv+u-v-11), \pm(-uv-u+v-11),\\ &\qquad \pm(-uv+3u+3v+11), \pm(-uv-3u-3v+11)\}\}.\end{aligned} \tag{4}$$

Equivalently, putting

$$\begin{aligned}f(T, u, v) = {}&(T^2 - (4(u+v))^2)(T^2 - (uv+u+v-11)^2)\\ &\cdot(T^2 - (uv-u-v-11)^2)\cdot(T^2 - (uv+3u-3v+11)^2)\\ &\cdot(T^2 - (uv-3u+3v+11)^2),\end{aligned}$$

then, using $(1')$, $f(T, u, v) - f(T, u, -v)$ is independent of T. To show that the sets of m_i's and n_i's are not the same, it is therefore enough to show that $f(0, u, v) \neq f(0, u, -v)$. This is readily shown, with the help of (3), to be equivalent to showing that

$$uv(u^2 - v^2)(u^2 - 9v^2)(9u^2 - v^2) \neq 0. \tag{5}$$

Since $uv(u^2 - v^2) \neq 0$ for rational solutions, and $u^2 = 9v^2$ implies that $(u, v) = (\pm 3, \pm 1)$ or $(\pm 11, \pm 11/3)$, we see that (5) holds, and so the sets $\{m_i\}$ and $\{n_i\}$ of (4) are distinct unless (u, v) is one of these eight pairs, or the eight pairs with the values u and v interchanged.

The solution $(n, p, q, m) = (51, 61, 573, 79)$, i.e., $u = \frac{153}{61}$, $v = \frac{191}{79}$, obtained by Letac [4, p. 55] gives the multigrade (see also [9, 6])

$$\begin{aligned}&\{\{\pm 12, \pm 11881, \pm 20231, \pm 20885, \pm 23738\},\\ &\quad \{\pm 436, \pm 11857, \pm 20449, \pm 20667, \pm 23750\}\}.\end{aligned} \tag{6}$$

We obtain this solution in a natural way in §6.

3. Rational solutions of $(u^2 - 13)(v^2 - 13) = 48$

Writing (3) projectively as

$$(U^2 - 13W^2)(V^2 - 13W^2) = 48W^4, \tag{3'}$$

we check that its singularities consist of ordinary double points at $(1, 0, 0)$ and $(0, 1, 0)$. Thus, the genus formula

$$g = \tfrac{1}{2}(d-1)(d-2) - \sum_j \tfrac{1}{2} r_j(r_j - 1)$$

[3, p. 199] for a plane curve of genus g, degree d, and only ordinary multiple points of multiplicity r_j, shows that $g = 1$. The curve, having a rational point, is therefore birationally equivalent to an elliptic curve in Weierstrass form. Indeed, using the standard technique described in [1, p. 212] or [7, p. 40], we can put

$$X = \frac{3u+v}{(u-1)(v-3)}, \qquad Y = \frac{13(79u - 191)}{37uv - 117u - 91v + 279}.$$

Then the only pole of X on (3) is the double pole at $(1, 3)$, while the only pole of Y on (3) is a triple pole at $(1, 3)$. Further,

$$Y^2 = -6X^3 - 83X^2 + \tfrac{29}{2}X + 7 + \tfrac{3}{2}Y + 21XY,$$

and then the substitution

$$X = (327 - x)/216, \qquad Y = (21573 - y - 63x)/1296 \tag{7}$$

gives

$$y^2 = x^3 - 556011x + 159551910 \tag{8}$$

or

$$y^2 = (x - 435)(x - 426)(x + 861).$$

(Equation (8) can also be derived from (3) by ad hoc methods, e.g., by first writing (3) as $(u(v^2 - 13))^2 = (13v^2 - 121)(v^2 - 13)$, and then using well-known tricks.)

Now under these transformations, $(u, v) = (3, 1)$ maps to $(X, Y) = (-\frac{5}{2}, -\frac{23}{2})$, and so maps to $(x, y) = (867, -18144)$ $(= P$ say). We can then use the tangent to (8) at P to give us another point Q $(= -2 \cdot P$ under the group law) where it meets the curve again. In fact,

$$Q = \left(\frac{359265}{784}, \frac{21829905}{21952}\right).$$

This point Q on (8) corresponds on the original curve (3) to the point

$$(u, v) = \left(\frac{-1264969}{424999}, \frac{-296313}{249661}\right),$$

which, using (4), gives the multigrade system

$$\begin{aligned} \{n_1, \dots, n_{10}\} &= \{\pm 133225698289, \pm 189880696822, \pm 338027122801, \\ &\qquad \pm 432967471212, \pm 529393533005\}, \\ \{m_1, \dots, m_{10}\} &= \{\pm 87647378809, \pm 243086774390, \pm 308520455907, \\ &\qquad \pm 441746154196, \pm 527907819623\}. \end{aligned} \tag{9}$$

Since $\gcd(n_1, n_5) = 1$, this is not a multiple of Letac's multigrade. It appears to be new, and is probably the smallest multigrade, apart from (6), obtainable by Letac's method.

Now, as Lutz and Nagell showed [5; 1, p. 264; 7, p. 221], every point of finite order on an elliptic curve $y^2 = x^3 - Ax + B$ with $A, B \in \mathbb{Z}$ has integer coordinates. Hence, Q has infinite order in the Mordell-Weil group on (8), and so (8) has infinitely many rational solutions.

The rational map $(u, v) \mapsto (x, y)$ described above has a rational inverse, which can be described explicitly as follows: map $(x, y) \mapsto (X, Y)$ by (7), and then put

$$\begin{aligned} c &= 1027x + 6XY - 111Y, & d &= -1027 - 3510X + 156Y - 12XY, \\ e &= 2483(1+X) + 279Y + 6XY, & L &= 9(X+1)^2 - 13X^2, \\ M &= 9X^2 - 13(X+1)^2, & R &= e + 13c, \\ V &= X^2 d + 2X(X+1)c, & W &= Le - Mc, \\ U &= Ld - 8X(X+1)c, & Z &= X^2 e - (X+1)^2 c. \end{aligned}$$

Then

$$u = \frac{dUe - RWc - 48c^2 Z}{-d^2U + cRU + cdW + 48c^2 V}$$

and

$$v = 3\left(\frac{(X+1)u - X}{Xu - (X+1)}\right).$$

Hence, infinitely many rational solutions (x, y) of (8) give infinitely many rational solutions (u, v) of (3).

4. An infinity of multigrades

We now show that the infinity of rational solutions of (3) give an infinity of genuinely different solution sets for (1). First, note that any affine map $ax + b$ connecting two multigrades given by (4) must have $b = 0$. This is clear, since these multigrades are symmetric about zero.

For any solution (u, v) of (3), the left and right solution sets $\{n_1, \dots, n_{10}\}$ and $\{m_1, \dots, m_{10}\}$ given by (4) can each be placed in ascending order. In doing this, we are clearly choosing one of $10!^2$ possible pairs of orderings. Hence if we have more than $5 \times 10!^2$ different solutions (u, v) of (3), at least five solutions $(u^{(k)}, v^{(k)})$ of (3) will give five solution sets $\{\{n_1^{(k)}, \dots, n_{10}^{(k)}\}, \{m_1^{(k)}, \dots, m_{10}^{(k)}\}\}$ $(k = 1, \dots, 5)$ which are in the same order relative to the parametrization (4) of these sets. So, for some i and j,

$$(10) \qquad 4(u^{(k)} + v^{(k)}) = n_i^{(k)}, \quad 4(u^{(k)} - v^{(k)}) = m_j^{(k)} \qquad (k = 1, \dots, 5).$$

Confining our attention to these five solution sets, and supposing that no two of the five are genuinely different, we would have

$$(11) \qquad n_i^{(k)} = a^{(k)} n_i^{(1)}, \quad m_j^{(k)} = a^{(k)} m_j^{(1)} \qquad (k = 1, \dots, 5),$$

so that (10) with (11) would give

$$u^{(k)} = a^{(k)}u^{(1)}, \quad v^{(k)} = a^{(k)}v^{(1)} \qquad (k = 1, \dots, 5).$$

But then

$$((a^{(k)}u^{(1)})^2 - 13)((a^{(k)}v^{(1)})^2 - 13) = 48 \qquad (k = 1, \dots, 5),$$

giving a quartic in $a^{(k)}$ with five different solutions. This being impossible, we have shown that any set of N solutions of (3) will give at least $N/(5 \times 10!^2)$ genuinely different solution sets of (1). (Further, if none of these are the sixteen solutions $(u, v) = (\pm 1, \pm 3), \dots$ mentioned in §2, these sets will also have $\{n_1, \dots, n_{10}\} \neq \{m_1, \dots, m_{10}\}$.) Hence, we certainly obtain, from an infinite number of solutions of (3), an infinite number of genuinely different solution sets of (1).

The constant $5 \times 10!^2$ in the above argument was chosen to make the argument simple, and is certainly not best possible. A more complicated argument, which will not be given here, shows that the best constant is in fact 16. For a given solution (u, v) of (3), the sixteen solutions $(\pm u, \pm v)$, $(\pm v, \pm u)$, $(\pm 11/u, \pm 11/v)$, $(\pm 11/v, \pm 11/u)$ all give the same multigrade.

5. The Mordell-Weil group of the curve

It is possible, by standard methods, to compute the Mordell-Weil group G of the curve (3), and hence compute all 9th-order ideal multigrades which can be produced by Letac's method. The result is that $G \cong C_2 \times C_4 \times C_\infty$, so that the curve has rank 1. In the original form (3), with $(1, 3)$ as the zero element, generators for each cyclic component can be taken as $(-11, -\frac{11}{3})$, $(3, -1)$, and $(3, 1)$, respectively. The precise form of the group law on (3), without reference to (8), is described in §6. For the curve in Weierstrass form (8), the corresponding generators are $(426, 0)$, $(543, -4212)$, and $(867, -18144)$.

We compute G using the form (8). We first find the torsion part G_{tors} of G. Since $(426, 0)$ and $(543, -4212)$ generate a group $\cong C_2 \times C_4$, we need only check that there are no more than eight points of finite order. This follows from the fact that, since (8) has discriminant $2^{12}3^{16}11^2 13$, (8) has good reduction at the prime 5. Hence [7, p. 176], there is an injection $G_{\text{tors}} \to G_5$, the group of (8) over $GF(5)$. But G_5 has eight elements also, so $G_{\text{tors}} \cong C_2 \times C_4$.

To find the torsion-free part of G, we compute $G/2G$, following [7, pp. 281–284]. The procedure is not guaranteed to work, but does so provided that for each of the finite number of "2-coverings" ((14), below) of the curve, one can either exhibit a rational point on the 2-covering, or show that it has no such point. The algorithm for a curve

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \tag{12}$$

with integral 2-division points $(e_i, 0)$ $(i = 1, 2, 3)$ is as follows: Let S be the set consisting of -1 and the primes p dividing the discriminant

$16(e_1-e_2)^2(e_2-e_3)^2(e_3-e_1)^2$ of (12), and $\mathbb{Q}_S$ be the (multiplicative) subgroup of $\mathbb{Q}^*$ generated by S and $\mathbb{Q}^{*2}$. Then the map φ from the curve given by (12) to $\mathbb{Q}_S/\mathbb{Q}^{*2}\times\mathbb{Q}_S/\mathbb{Q}^{*2}$ defined by

$$(13)\qquad (x, y)\overset{\varphi}{\mapsto}((x-e_1)\mathbb{Q}^{*2}, (x-e_2)\mathbb{Q}^{*2})$$

is an injective homomorphism (this property is used to define φ at ∞, $(e_1, 0)$, and $(e_2, 0)$ where (13) is not applicable). Its image consists of points $(d_1\mathbb{Q}^{*2}, d_2\mathbb{Q}^{*2})$ with $d_1, d_2\in\mathbb{Q}_S$ for which the 2-covering

$$(14)\qquad \begin{cases} d_1z_1^2-d_2z_2^2=e_2-e_1, \\ d_1z_1^2-d_1d_2z_3^2=e_3-e_1 \end{cases}$$

of (8) has a rational point (z_1, z_2, z_3). The pre-image (x, y) on (8) of $(d_1\mathbb{Q}^{*2}, d_2\mathbb{Q}^{*2})$ under φ is then $(e_1+d_1z^2, d_1d_2z_1z_2z_3)$.

Following [7], one can show that for the particular curve (8), $\operatorname{Im}\varphi$ is generated by $(\mathbb{Q}^{*2}, 3\mathbb{Q}^{*2})=\varphi(867, -18144)$, $(-11\mathbb{Q}^{*2}, -\mathbb{Q}^{*2})=\varphi(327, -3564)$, and $(13\mathbb{Q}^{*2}, \mathbb{Q}^{*2})=\varphi(439, -260)$. (These points correspond to the points $(u, v)=(3, 1), (-\frac{11}{3}, 11)$, and $(1, -3)$, respectively, on the original curve (3).) Two of these generators are accounted for by the image of $G_{\text{tors}}/2G$, which is generated by $(13\mathbb{Q}^{*2}, 3\mathbb{Q}^{*2})$ and $(-11\times 13\mathbb{Q}^{*2}, -\mathbb{Q}^{*2})$. Hence, G has a single generator of infinite order: $G\cong C_2\times C_4\times C_\infty$.

The proof that the above three points generate $\operatorname{Im}\varphi$ is obtained by verifying first that, for (8), the 2-covering (14) has no solution with $(d_1, d_2)=(-1, -1), (1, 2)$, or $(-1, -2)$. One also checks that for $(d_1\mathbb{Q}^{*2}, d_2\mathbb{Q}^{*2})\in\operatorname{Im}\varphi$, we have $\operatorname{Sgn}d_1=\operatorname{Sgn}d_2$, $2\nmid d_1$, $3\nmid d_1$, $11\nmid d_2$, and $13\nmid d_2$. Each of these facts is verified by a local argument at the relevant prime. The result then follows.

6. Solutions using tangent conics

Although solutions (u, v) of (3) can be found using the rational mapping $(x, y)\mapsto(u, v)$ described above, the procedure is somewhat cumbersome. The use of conics tangent to (3), however, provides a direct method of producing solutions of (3). This idea has recently been used by Elkies [2, p. 832].

The conic

$$(15)\qquad AUV+BUW+CVW+DW^2=0$$

meets the projective conic (3′) in eight points in the complex projective plane. Four of these intersections are at the two double points. If three of the remaining four points are rational, then the fourth will be also. In particular, if we take $A=37$, $B=-117$, $C=-91$, $D=279$ (i.e., the denominator of Y in §3), then three intersection points are at $(u, v)=(1, 3)$. The fourth intersection point is then $(\frac{191}{79}, -\frac{153}{61})$, providing one explanation of where Letac's solution of (3) comes from.

If we now take another conic merely tangent at $(1, 3)$ and passing through $(\frac{191}{79}, \frac{153}{61})$, we obtain a fourth point of intersection $(\frac{-1264969}{424999}, \frac{296313}{249661})$, which again gives the multigrade (9).

It is natural to expect that these conics (15) are connected with the group law on (3). Indeed, if $h(P_1, P_2, P_3) = P_4$, where P_1, P_2, P_3, P_4 are nonsingular points of $(3')$ lying on some conic (15), then group addition $+$ is defined by $P_1 + P_2 = h(0, 0, h(P_1, P_2, 0))$. Here, 0 is the zero of the group, which we take as $(1, 3, 1)$.

Acknowledgments

The author would like to thank Liam O'Carroll for correcting an error in one of the calculations on this problem, and Richard Pinch and Nelson Stephens for helpful discussions.

Added in proof. John Leech has informed me that the curve considered in this paper is connected with the problem of finding two rational right-angled triangles on the same base whose heights are in the ratio $k : 1$. The curve of this problem, $x - x^{-1} = k(y - y^{-1})$, is elliptic for $k \neq 0, \pm 1$, and for $k = 12$ has Weierstrass form (8). Leech showed that these curves have torsion group $C_2 \times C_4$ and, for integers $1 < k \leq 40$, have rank 0 or 1.

Bibliography

1. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **44** (1966), 193–291.
2. N. D. Elkies, *On* $A^4 + B^4 + C^4 = D^4$, Math. Comp. **51** (1988), 825–835.
3. W. Fulton, *Algebraic curves*, Benjamin, New York, 1969.
4. A. Gloden, *Mehrgradige Gleichungen*, Noordhoff, Groningen, 1944.
5. T. Nagell, *Solution de quelque problèmes dans la théorie arithmétique des cubiques planes du premier genre*, Vid. Akad. Skrifter Oslo **1** (1935), no. 1.
6. E. Rees and C. Smyth, *On the constant in the Tarry-Escott Problem*, Fifty Years of Polynomials, Lecture Notes in Math., vol. 1415, Springer, Berlin and New York, 1990, pp. 196–208.
7. J. H. Silverman, *The arithmetic of elliptic curves*, Springer, Berlin and New York, 1986.
8. E. M. Wright, personal communication, 1989.
9. ——, *The Tarry-Escott and the "easier" Waring problems*, J. Reine Angew. Math. **311/312** (1979), 170–173.

Department of Mathematics, University of Edinburgh, The James Clerk Maxwell Building, The King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, Scotland
E-mail address: C.Smyth@edinburgh.ac.uk